STUDIA I PRACE
Kolegium Zarządzania i Finansów
ZESZYT NAUKOWY 157

157/2017
s. 9–30

Szkoła Główna Handlowa w Warszawie
Oficyna Wydawnicza SGH
kolegia.sgh.waw.pl

Elżbieta Izabela Szczepankiewicz
Katedra Rachunkowości
Uniwersytet Ekonomiczny w Poznaniu

Zagrożenia dla zasobów informatycznych rachunkowości w dobie transformacji *Information Technology* w jednostkach sektora finansów publicznych

Streszczenie

Ważnym aspektem właściwego poziomu sprawności i jakości działania w jednostkach sektora finansów publicznych jest zapewnienie ciągłości działania systemów informatycznych i bezpieczeństwa zasobów informatycznych. Wykorzystanie systemów informatycznych i techniki teleinformatycznej w tych jednostkach wiąże się z wieloma zagrożeniami związanymi ze środowiskiem informatycznym. W opracowaniu omówiono najważniejsze zagrożenia, które dotyczą tradycyjnego modelu zarządzania zasobami informatycznymi w jednostkach oraz nowego modelu „przetwarzania w chmurze" (ang. *cloud computing*). Poruszono problem zagrożeń i zaprezentowano wnioski z badań w kontekście transformacji technologicznych oraz niedoskonałości systemów kontroli zarządczej, które nie zawsze nadążają za tymi zmianami. Metodą badawczą przyjętą w opracowaniu jest przegląd literatury, przepisów prawnych, standardów kontroli zarządczej, standardów audytu wewnętrznego, norm ISO oraz wnioskowanie.

Słowa kluczowe: rachunkowość, system informatyczny, zagrożenia, bezpieczeństwo zasobów IT, zarządzanie ryzykiem, system kontroli zarządczej, *cloud computing*
Kod klasyfikacji JEL: M15

1. Wprowadzenie

Od wielu lat zarządzanie w jednostkach sektora finansów publicznych (JSFP) wspomagane jest rozwiązaniami i narzędziami informatycznymi. Jednym z najważniejszych aspektów sprawności działania tych jednostek jest zapewnienie ciągłości działania systemów informatycznych rachunkowości oraz wiarygodności i bezpieczeństwa informacji finansowej.

Współczesne uwarunkowania funkcjonowania JSFP powodują, że skuteczne zarządzanie środowiskiem informatycznym w JSFP staje się coraz trudniejsze. Od kilku lat systematycznie rośnie liczba zagrożeń związanych z wykorzystaniem nowych rozwiązań informatycznych i transformacji technologii w tym zakresie. Powszechnie mówi się o różnego rodzaju masowych cyberatakach na publiczne bazy danych, zarówno dużych, jak i małych JSFP[1].

Poza incydentami dotyczącymi bezpieczeństwa informacji w JSFP należy mieć na uwadze także wiele innych czynników ryzyka, które mogą zagrażać pozostałym zasobom w środowisku informatycznym, w tym tych, które są związane z prowadzeniem zinformatyzowanej rachunkowości. Dlatego w ostatnich latach w praktyce sektora finansów publicznych coraz większą uwagę przywiązuje się do poprawienia skuteczności zarządzania ryzykiem w środowisku informatycznym rachunkowości w ramach funkcjonujących w tych jednostkach systemów kontroli zarządczej. Szczególnie ważne dla obszaru funkcjonowania systemów informatycznych rachunkowości w JSFP są zasady i procedury kontroli zarządczej, które dotyczą zapewnienia: poprawności przetwarzania danych finansowych, wiarygodności ksiąg rachunkowych oraz sprawozdań finansowych i budżetowych, a także bezpieczeństwa pozostałych zasobów informatycznych rachunkowości.

[1] Z różnych raportów instytucji specjalistycznych, monitorujących incydenty bezpieczeństwa informatycznego, a także z informacji medialnych, wynika, że wiele JSFP codziennie odnotowuje nawet po kilkanaście lub kilkadziesiąt prób ataków na ich zasoby informacji.

Ze względu na stopień skomplikowania i interdyscyplinarność tematu (wymaga on znajomości organizacji rachunkowości w środowisku informatycznym, różnych zagadnień z zakresu informatyki, zarządzania ryzykiem, właściwej interpretacji wielu różnorodnych tematycznie regulacji w przedmiotowym obszarze) w krajowej literaturze naukowej, poza kilkoma opracowaniami autorki, temat ten jest bardzo rzadko naświetlany. Naukowcy w Polsce nie prowadzili dotychczas badań empirycznych w tym zakresie. Należy podkreślić, że Stowarzyszenie do spraw Audytu i Kontroli Systemów Informatycznych (ISACA) obecnie jest w trakcie opracowywania pierwszego raportu na temat bezpieczeństwa informacji i cyberbezpieczeństwa w jednostkach sektora finansów publicznych, które ma się ukazać w 2017 r. Zatem wiedza teoretyczna i praktyczna pozostaje nadal zasobem prywatnym praktyków w JSFP.

Z powyższych względów podstawowym celem opracowania jest uporządkowanie teoretycznych i praktycznych aspektów wiedzy o elementach środowiska informatycznego rachunkowości oraz o ich podatności na zagrożenia we współczesnej cyberprzestrzeni jednostek funkcjonujących w sektorze finansów publicznych w kontekście realizacji celów kontroli zarządczej[2]. W opracowaniu omówiono najważniejsze czynniki ryzyka w tradycyjnym modelu zarządzania zasobami informatycznymi w JSFP oraz przy wykorzystaniu nowych modeli *cloud computing*. Zaprezentowano również wyniki przeprowadzonych badań empirycznych na temat zagrożeń i oceny stanu ochrony przed nimi w ramach systemów kontroli zarządczej w JSFP.

2. Formalne aspekty zarządzania bezpieczeństwem zasobów informatycznych rachunkowości w jednostkach sektora finansów publicznych

Od wielu lat ogólne zasady bezpieczeństwa zasobów informatycznych oraz zapewnienia wiarygodności przetwarzania danych i informacji finansowej pochodzącej z systemu informatycznego rachunkowości we wszystkich jednostkach, które prowadzą rachunkowość zgodnie z przepisami ustawy o rachunkowości, są regulowane zapisami tejże ustawy. Podstawowe przepisy prawa bilansowego w zakresie ochrony danych i systemu informatycznego rachunkowości dotyczą:

[2] Artykuł powstał w ramach projektu międzyuczelnianego nr 51109-XX4 „Doskonalenie procesów zarządzania ryzykiem w jednostkach sektora finansów publicznych i jednostkach sektora finansowego. Metody, techniki, narzędzia", realizowanego w UE w Poznaniu pod kierownictwem dr E.I. Szczepankiewicz.

- wymagań ochrony danych, które wynikają z art. 10, 13, 23, 24, 71 i 72 ustawy,
- warunków przechowywania ksiąg rachunkowych w formie zbiorów na nośnikach komputerowych określonych w art. 72,
- stosowania zabezpieczeń fizycznych i organizacyjnych w jednostce, których obowiązek wynika z art. 71 ust. 2 ustawy,
- zapewnienia trwałości zapisu danych w systemie informatycznym rachunkowości, które wynika z art. 72 ust. 2 ustawy.

W JSFP zarządzanie środowiskiem informatycznym, w tym środowiskiem zinformatyzowanej rachunkowości, jest uwarunkowane nie tylko przepisami ustawy o rachunkowości, lecz także ustawy o finansach publicznych[3], standardami kontroli zarządczej[4], standardami audytu wewnętrznego[5], a także wieloma innymi przepisami[6] i normami ISO, dotyczącymi bezpieczeństwa informacji[7].

[3] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2013 r., poz. 885 z późn. zm.).

[4] Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz.Urz. Min. Fin. 2009, nr 15, poz. 84).

[5] Komunikat Nr 2 Ministra Finansów z dnia 17 czerwca 2013 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych (Dz.Urz. Min. Fin. z 2013 r., poz. 15).

[6] Do przepisów prawa w tym obszarze należy zaliczyć m.in.: ustawę o ochronie danych osobowych, ustawę o ochronie baz danych, ustawę o świadczeniu usług drogą elektroniczną, ustawę o podpisie elektronicznym, ustawę o ochronie osób i mienia, ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne. Do ustaw wydano także wiele aktów wykonawczych w tym zakresie: rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych; rozporządzenie w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty i warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego; rozporządzenie w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej; rozporządzenie w sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej; rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych; rozporządzenie w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych; rozporządzenie zmieniające rozporządzenie w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych; rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych; rozporządzenie zmieniające rozporządzenie w sprawie określenia rodzajów deklaracji, które mogą być składane za pomocą środków komunikacji elektronicznej; rozporządzenie zmieniające rozporządzenie w sprawie trybu dostępu i wzoru upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych.

[7] Najważniejsze normy ISO w jednostkach sektora finansów publicznych to na przykład: PN-ISO/IEC 17799/2007; PN-ISO/IEC 2382–8:2001; PN-I-02000:2002; PN-ISO/IEC 27001:2007; PN-ISO/IEC 27005:2014–01; PN-ISO/IEC 24762:2010; PN-ISO/IEC 20000–2:2007; PN-ISO/IEC 20000–1:2014–01.

Niewątpliwie, na jakość zarządzania środowiskiem informatycznym w danej JSFP ma także wpływ specyfika organizacji środowiska informatycznego oraz jakość stosowanych środków zabezpieczeń w tej jednostce. Specyfika organizacji środowiska informatycznego w danej jednostce głównie zależy od poziomu skłonności kierownictwa do ryzyka, natomiast jakość zastosowanych środków ochrony uwarunkowana jest zabezpieczeniem (zaplanowaniem i otrzymaniem) na te cele odpowiedniego poziomu środków budżetowych.

3. Elementy środowiska informatycznego rachunkowości

W polskiej literaturze nikt jeszcze nie zdefiniował środowiska informatycznego dla rachunkowości w JSFP ani nie wskazał jej elementów. Pojęcie to również nie zostało dotąd zdefiniowane w żadnych polskich przepisach i standardach dotyczących rachunkowości, standardach rewizji finansowej czy standardach audytu wewnętrznego. Nie zawarto również takiej definicji i nie opisano elementów środowiska informatycznego w standardach kontroli zarządczej, które bezpośrednio dotyczą tego obszaru zarządzania w JSFP. Należy wspomnieć, że w ustawie o rachunkowości ustawodawca używa takich terminów, jak: system informatyczny, system przetwarzania danych, informatyczny nośnik danych, system informatyczny rachunkowości. Terminy te jednak nie zostały zdefiniowane w tym akcie.

Definicję środowiska informatycznego można znaleźć jedynie w Międzynarodowych Standardach Rewizji Finansowej (MSRF)[8] z 1996 r. W myśl MSRF 401[9] środowisko systemów informatycznych istnieje, gdy komputer dowolnego typu i wielkości jest użytkowany do przetwarzania przez jednostkę informacji finansowych znaczących dla badania, niezależnie od tego, czy komputer ten obsługuje jednostka, czy

[8] *Międzynarodowe Standardy Rewizji Finansowej 1996*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 1996.

[9] Należy wspomnieć, że MSRF 401 zawarty w MSRF z 1996 r. usunięto ze struktury MSRF podczas ich aktualizacji w grudniu 2004 r., ale najważniejsze wytyczne z tego standardu zostały włączone w treść innych znowelizowanych standardów oraz nowo przyjętego MSRF 315 oraz *MSRF 315 – Poznanie jednostki i jej środowiska oraz szacowanie ryzyka wystąpienia istotnej nieprawidłowości*, w: *Międzynarodowe Standardy Rewizji Finansowej 2005. Wydanie zbiorcze obejmujące regulacje z zakresu rewizji finansowej, usług atestacyjnych i etyki*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 2005, a następnie zmodyfikowanego w 2009 r. *MSRF 315 Rozpoznanie i ocena ryzyka istotnego zniekształcenia dzięki poznaniu jednostki i jej otoczenia*, w: *Międzynarodowe Standardy Rewizji Finansowej i Kontroli Jakości: 210, 220, 240, 250, 265, 300, 315, 320, 402, 450, 800, 805, 810*, t. 3, IFAC, tłumaczenie: Krajowa Izba Biegłych Rewidentów i Stowarzyszenie Księgowych w Polsce, Warszawa 2010.

strona trzecia[10]. W 2001 r. do zaktualizowanych MSRF dodano *Słownik terminów IT*[11], w którym środowisko IT zdefiniowano jako zasady i procedury wdrożone przez jednostkę, a także infrastrukturę informatyczną, programy (aplikacje) użytkowe i bazy danych przez nią wykorzystywane przy prowadzeniu działalności jednostki.

Zatem należy wnioskować, że w JSFP przetwarzanie danych finansowych z wykorzystaniem oprogramowania dla rachunkowości oznacza, że odbywa się ono w środowisku informatycznym rachunkowości. Rozpatrując strukturę środowiska informatycznego dla systemu rachunkowości, można stwierdzić, że tworzą ją co najmniej takie kategorie, jak:

- zasoby informatyczne wykorzystane do prowadzenia rachunkowości,
- infrastruktura techniczna,
- personel, związany ze środowiskiem informatycznym rachunkowości, który można dzielić według różnych grup zawodowych,
- system organizacji pracy w jednostce,
- elementy otoczenia zewnętrznego.

W każdej z wyżej wymienionych kategorii związanej ze środowiskiem informatycznym rachunkowości można wskazać wiele elementów szczegółowych, które są z nimi związane. Przykładowo do zasobów informatycznych w JSFP zaliczyć należy przede wszystkim[12]:

- sprzęt komputerowy, tj. komputery, serwery, monitory, drukarki, modemy, skanery itd.,
- oprogramowanie systemowe, np. system operacyjny, system zarządzania bazą danych, narzędzia systemowe, programy diagnostyczne,
- oprogramowanie użytkowe uniwersalne, np. arkusze kalkulacyjne, edytory tekstów,
- oprogramowanie specjalne, czyli aplikacje użytkowe, w tym podsystemy dziedzinowe rachunkowości (np. system finansowo-księgowy, system gospodarki magazynowej, system kadrowo-płacowy),
- zbiory (bazy) danych, w tym bieżące kopie bezpieczeństwa danych oraz kopie ksiąg rachunkowych,

---

[10] Paragraf 1 *MSRF 401 – Badanie w środowisku komputerowych systemów informacyjnych*, w: *Międzynarodowe Standardy Rewizji Finansowej i Międzynarodowe Wskazówki dotyczące Praktyki Rewizji Finansowej 2001*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 2001, s. 187.

[11] *Słownik terminów IT*, w: *Międzynarodowe Standardy Rewizji...*, op.cit., s. 720.

[12] E.I. Szczepankiewicz, *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych*, red. W. Gabrusewicz, PWE, Warszawa 2010, s. 198.

- nośniki danych,
- dokumentację projektową rozwiązań informatycznych, w tym rozwoju (i/lub aktualizacji funkcji) systemu informatycznego rachunkowości,
- dokumentację ewidencyjną systemu informatycznego rachunkowości,
- dokumentację dla użytkowników systemu informatycznego rachunkowości.

Infrastrukturę techniczną w JSFP tworzą systemy zasilania, chłodzenia, klimatyzacji, ochrony przeciwpożarowej, sieci teletransmisyjne i centra administracyjne systemu, systemy (procedury) ochrony dostępu fizycznego do zasobów informatycznych itp.[13].

Personel związany ze środowiskiem informatycznym rachunkowości w JSFP można dzielić według grup zawodowych, czyli są to: użytkownicy podsystemów rachunkowości (tj. osoby prowadzące ewidencję operacji, inne osoby kadry księgowej, kierowniczej, osoba administrująca uprawnieniami użytkowników), projektanci systemów informatycznych, programiści systemów informatycznych, oficer bezpieczeństwa, zewnętrzni programiści podsystemów rachunkowości, administratorzy systemów i/lub baz danych, serwisanci sprzętu komputerowego, serwisanci oprogramowania, osoby odpowiedzialne za dystrybucję i bezpieczeństwo nośników danych[14].

Mając na uwadze system organizacji pracy w JSFP, mówimy o scentralizowanym lub rozproszonym przetwarzaniu danych, które jest realizowane we własnym zakresie przez jednostkę, albo o powierzeniu prowadzenia rachunkowości innej jednostce (może to dotyczyć małych JSFP), a także o korzystaniu z usług specjalistycznych centrów administrowania danymi. Z tym zagadnieniem wiąże się odpowiednia organizacja systemu kontroli zarządczej w danej JSFP i podział odpowiedzialności za kontrolę nad zasobami informatycznymi.

Do elementów otoczenia zewnętrznego, który ma wpływ na zakres procedur kontroli zarządczej w JSFP, zaliczyć należy co najmniej[15]:

- organizację przetwarzania danych przy powierzeniu prowadzenia rachunkowości lub przetwarzania innych danych jednostce zewnętrznej,

---

[13] E.I. Szczepankiewicz, *Zasady i procedury kontroli zarządczej w obszarze systemów informatycznych rachunkowości w jednostkach sektora finansów publicznych*, Wydawnictwo Naukowe CONTACT, Poznań 2016, s. 19.

[14] E.I. Szczepankiewicz, *Kontrola zarządcza w jednostkach samorządu terytorialnego. Doskonalenie procedur kontroli zarządczej w środowisku informatycznym rachunkowości*, Wydawnictwo Naukowe CONTACT, Poznań 2016, s. 28.

[15] E.I. Szczepankiewicz, *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych. Teoria i praktyka*, red. W. Gabrusewicz, PWE, Warszawa 2014, s. 232.

- organizację przekazywania danych pomiędzy jednostkami sektora publicznego lub między JSFP a inną jednostką zewnętrzną (forma tradycyjna lub przy użyciu łącz transmisyjnych, np. przez Internet),
- podział odpowiedzialności za kontrolę i bezpieczeństwo danych między stronami powyższych umów.

Wyżej wymienione elementy szczegółowe środowiska informatycznego rachunkowości występują w mniejszym lub większym zakresie w każdej JSFP, niezależnie od jej formy organizacyjnej, wielkości, zakresu realizowanych zadań publicznych czy specyfiki działania. Powyższe elementy środowiska informatycznego są charakterystyczne także dla innych jednostek gospodarczych w sektorze prywatnym.

4. Czynniki ryzyka w środowisku informatycznym rachunkowości

Cechy środowiska informatycznego oraz podatność jego poszczególnych elementów na różnego typu zagrożenia w JSFP wiążą się z jakością wykorzystywanego systemu informatycznego rachunkowości, a także z charakterem organizacji systemu rachunkowości oraz systemu kontroli zarządczej w jednostce.

W JSFP zwraca się szczególną uwagę na te elementy środowiska informatycznego i zagrożenia z nimi związane, które mogą wywoływać negatywne efekty dla prawidłowego działania i bezpieczeństwa zasobów informatycznych rachunkowości oraz bezpieczeństwa informacji w publicznych bazach danych. Źródłami ryzyka w JSFP mogą być różne elementy środowiska informatycznego[16]. Jak wyżej wskazano, mogą to być poszczególne elementy zasobów informatycznych, personel księgowy i informatyczny, sposób organizacji pracy i kontroli, a także otoczenie zewnętrzne. Należy jednak pamiętać o tym, że nie wszystkie zagrożenia związane z poszczególnymi elementami środowiska informatycznego w jednakowy sposób mogą oddziaływać

[16] Szerzej o zagrożeniach w środowisku informatycznym: E. Dudek, *Zagrożenia występujące w środowisku informatycznym rachunkowości*, „Monitor Rachunkowości i Finansów" 2003, nr 7–8, s. 45–52; E.I. Szczepankiewicz, M. Dudek, *Rozwój technologii informatycznych a zagrożenia i zarządzanie bezpieczeństwem informacji w przedsiębiorstwach*, w: *Logistyka – Komunikacja – Bezpieczeństwo, Wybrane problemy*, red. M. Grzybowski, J. Tomaszewski, Wydawnictwo Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni, Gdynia 2009, s. 263–274.

na bezpieczeństwo zasobów informatycznych i prawidłowe funkcjonowanie systemu informatycznego rachunkowości[17].

Czynniki ryzyka w środowisku informatycznym teoretycy najczęściej klasyfikują według rodzajów oraz według skutków[18]. Wielu autorów wskazuje, że dane zagrożenie może być spowodowane przez: działanie czynników środowiska naturalnego (zdarzenia losowe) oraz przypadkowe lub celowe działania człowieka, które w efekcie spowodują szkody w zasobach informatycznych jednostki. Zdarzenia losowe, a także przypadkowe lub celowe działania ludzi mogą być pochodzić zarówno z wewnątrz, jak i z zewnątrz jednostki. Zatem na środowisko informatyczne rachunkowości w JSFP mogą mieć wpływ różne wewnętrzne i zewnętrzne czynniki ryzyka.

Wiele wyników badań wskazuje, że pomimo zmieniających się warunków otoczenia i postępu technologii w dziedzinie informatyki, głównym źródłem ryzyka w JSFP, podobnie jak w innych jednostkach gospodarczych, są ludzie związani z systemem informatycznym rachunkowości lub z jego otoczeniem, którzy bezpośrednio lub pośrednio, przypadkowo lub umyślnie wpływają na działanie systemu i/lub bezpieczeństwo informacji[19].

Do celowych działań człowieka przeciwko zasobom informatycznym zgodnie z klasyfikacją normy ISO/IEC TR 13335–3 zalicza się m.in.: zalanie, pożar, umyślną szkodę lub zniszczenie, awarię klimatyzacji, ekstremalną temperaturę i wilgotność, promieniowanie elektromagnetyczne, kradzież, nieuprawnione użycie nośników, błędy personelu obsługującego / użytkowników, nielegalne używanie oprogramowania, błąd konserwacji/serwisu oprogramowania, awarię oprogramowania, użycie oprogramowania przez nieuprawnionych użytkowników, sfałszowanie tożsamości użytkownika, instalację złośliwego oprogramowania, dostęp do sieci nieuprawnionych użytkowników, użycie instalacji sieciowych w nieuprawniony sposób, uszkodzenie linii telekomunikacyjnych, przeciążenie ruchem, podsłuch, infiltrację łączności, analizę ruchu, przekierowanie wiadomości, zaprzeczenie, awarię usług łączności (np. usług sieciowych), niewłaściwe wykorzystanie zasobów informatycznych, a nawet atak terrorystyczny czy użycie broni do zniszczenia zasobów informatycznych.

---

[17] E.I. Szczepankiewicz, *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych. Teoria i praktyka...*, op.cit., s. 234.

[18] Klasyfikacje zagrożeń według tych kryteriów proponują na przykład: R.P. Fisher, *Information Systems Security*, Prentice-Hall, Englewood Cliffs 1984, s. 54; T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Helion, Gliwice 1999, s. 24–25.

[19] Szerzej szczegółowe wyniki badań o zagrożeniach w środowisku informatycznym rachunkowości prezentują: E.I. Szczepankiewicz, M. Dudek, *Rozwój technologii...*, op.cit., s. 263–274.

Szczególną kategorią celowego działania w środowisku informatycznym JSFP jest przestępczość komputerowa, prowadząca do naruszenia bezpieczeństwa zasobów informatycznych. Działania przestępcze mogą być skierowane przeciwko dostępności informacji, integralności lub jej poufności. Są to na przykład takie działania, jak: haking, fishing, rozpowszechnianie wirusów, niszczenie informacji, wandalizm, kradzież danych lub sprzętu, wewnętrzny lub zewnętrzny sabotaż komputerowy, oszustwo komputerowe, fałszerstwo komputerowe, szpiegostwo komputerowe, podsłuch komputerowy, nielegalne uzyskiwanie i wykorzystywanie programu. Zazwyczaj większość tych działań pochodzi z zewnątrz JSFP. Działania te znalazły odzwierciedlenie w przepisach prawa karnego i prawa o wykroczeniach[20].

Podstawowe zagrożenia dotyczące tradycyjnego modelu zarządzania zasobami informatycznymi, czyli takiego, gdzie JSFP posiada własną infrastrukturę informatyczną i na bieżąco sama utrzymuje ciągłość działania sprzętu komputerowego, w tym serwerów (zasilanie, chłodzenie, serwisowanie itp.), oprogramowania, infrastruktury sieciowej, dotyczą niedoskonałości systemu kontroli zarządczej. Zagrożenia te można podzielić na kilka grup.

Pierwszą grupę zagrożeń stanowią braki i/lub niedoskonałości w zakresie stosowanych zabezpieczeń fizycznych, technicznych i programowych dla zasobów informatycznych i/lub brak ubezpieczenia tych zasobów od zdarzeń losowych. W tej grupie ważne są również aspekty zabezpieczenia się przed zagrożeniami, wynikającymi z niewłaściwej konfiguracji lub stosowania nieodpowiednich zabezpieczeń, dotyczących lokalnych sieci komputerowych w jednostce. Jest to zagrożenie występujące najczęściej w mniejszych JSFP. Błędy i braki w tym zakresie mogą prowadzić m.in. do wewnętrznych i zewnętrznych nadużyć czy przestępstw komputerowych.

Drugą grupę czynników ryzyka w JSFP stanowią braki i/lub niedoskonałe wewnętrzne procedury organizacyjno-administracyjne, które mogą być wykorzystywane przez pracowników do celowych, wewnętrznych naruszeń wobec zasobów informatycznych. W JSFP, podobnie jak w innych jednostkach gospodarczych, bezpośrednio na środowisko informatyczne rachunkowości negatywnie mogą oddziaływać użytkownicy podsystemów informatycznych rachunkowości (kierownictwo, kasjerzy, pozostały personel księgowy), zatrudnieni w jednostce programiści itd. Może to być każda osoba, która uczestniczy w funkcjonowaniu (eksploatacji) systemu,

[20] J.W. Wójcik, *Przestępstwa komputerowe*, cz. 1, *Fenomen cywilizacji*, CIM, Warszawa 1999; J.W. Wójcik, *Przestępstwa komputerowe*, cz. 2, *Techniki zapobiegania*, CIM, Warszawa 1999; K. Mitnick, W. Simon, *Łamałem ludzi, nie hasła. Sztuka podstępu*, Helion, Gliwice 2002; Ustawa z 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r., nr 55, poz. 553 z późn. zm.).

dokładnie znająca ten system oraz niedoskonałości mechanizmów kontroli. Mogą to być także osoby działające indywidualnie lub w zmowie, które mogą zmodyfikować programy albo dane podczas ich wprowadzania i/lub przechowywania. Niebezpieczeństwo takie istnieje szczególnie wtedy, gdy nie występuje skuteczna kontrola zarządcza oparta na właściwym podziale: upoważnień, autoryzacji, funkcji i zadań w strukturze organizacyjnej JSFP.

Groźnym zagrożeniem dla wiarygodności systemu informatycznego rachunkowości w JSFP może być fakt pominięcia testowania systemu informatycznego rachunkowości przed przyjęciem go do eksploatacji, w szczególności w przypadku rozwiązania indywidualnie zamawianego przez jednostkę. Brak takiego testowania stanowi dodatkowy element ryzyka pojawienia się błędów w późniejszym przetwarzaniu danych i sprawozdawczości w jednostce.

Kolejnym bardzo ważnym czynnikiem ryzyka jest brak zaprogramowanych automatycznych procedur kontrolnych w systemach (aplikacjach) użytkowych. W praktyce JSFP systemy informatyczne rachunkowości, w zależności od ceny i klasy systemu, mają bardzo różny poziom i liczbę zaprogramowanych procedur kontrolnych. Niewątpliwie procedury kontroli zarządczej[21] w systemie informatycznym rachunkowości mogą i powinny być realizowane programowo. Jeśli przewidzi się odpowiednie mechanizmy kontroli, w zbiorach danych zapisywane są tylko operacje spełniające warunki kontroli, natomiast treści błędne są na ogół odrzucane przez system już na etapie wprowadzania danych do komputerowego dokumentu księgowego. Ponadto użytkownik, obsługując system informatyczny rachunkowości z zaprogramowanymi kontrolami poprawności wprowadzania danych, może na bieżąco uzyskiwać pomoc (podpowiedzi) ze strony systemu podczas ewidencji operacji księgowych i korzystać z wcześniej wprowadzonych do systemów wzorców księgowań[22].

Wraz z rozwojem JSFP może zaistnieć konieczność zainwestowania w dodatkową infrastrukturę informatyczną. Wówczas jednostka powinna rozważyć, czy nadal będzie tradycyjnie zarządzać swoimi zasobami informatycznymi, ponosząc pełne koszty z tym związane, czy może będzie korzystać z tzw. modelu „przetwarzania

[21] Szerzej o procedurach kontrolnych E.I. Szczepankiewicz, *Wybrane procedury kontroli wewnętrznej w środowisku informatycznym rachunkowości*, w: *Rachunkowość w teorii i praktyce*, t. I, *Rachunkowość finansowa*, red. W. Gabrusewicz, Wydawnictwo Akademii Ekonomicznej w Poznaniu, Poznań 2007, s. 360–376; E.I. Szczepankiewicz, *Jakie są zasady opracowywania procedur kontrolnych w firmie*, „Biuletyn Rachunkowości" 2008, nr 12(60), s. 58–60.

[22] Szerzej E. Dudek, *Zagrożenia*..., op.cit., s. 46.

w chmurze" (ang. *cloud computing*). Należy przewidzieć, że nowe rozwiązania technologiczne operujące w cyberprzestrzeni, pomimo że są tańsze niż utrzymywanie własnej pełnej infrastruktury i personelu informatycznego, będą źródłem dodatkowych nowych zagrożeń dla zasobów informatycznych jednostki.

Przetwarzanie w chmurze to świadczenie określonych, specjalistycznych usług informatycznych za pośrednictwem infrastruktury sieciowej (Internetu). Jest to usługa przetwarzania danych. Poprzez dostęp sieciowy usługodawca na bieżąco (*online*) dostarcza usługobiorcom współdzielony z wieloma usługobiorcami zestaw zasobów przetwarzania, czyli sieci, serwery, przestrzeń do składowania danych, oprogramowanie i usługi z tym związane. Zatem „chmurę" stanowi cały zbiór serwerów, oprogramowania, światłowodów itd., do którego uzyskuje się dostęp za pośrednictwem Internetu. Korzystanie z takiej chmury nazywa się „przetwarzaniem w chmurze"[23]. Usługobiorca, korzystając z tej usługi, nie musi mieć wiedzy technicznej o tym, w jaki sposób odbywa się cały proces dostarczania usługi. Nie wie również, w której części globu fizycznie znajdują się poszczególne elementy całej zaawansowanej technologicznie infrastruktury informatycznej dla tej usługi, w tym: serwery z zasobami informacyjnymi, z których on na co dzień korzysta. Usługa przetwarzania w chmurze ma charakter mierzalny (liczba przesłanych bajtów, czas korzystania itp.). Dlatego usługobiorca płaci tylko za rzeczywiste korzystanie z zasobów[24].

W zależności od stopnia zaawansowania *cloud computing* rozróżnia się obecnie trzy podstawowe rodzaje/poziomy tej usługi:

1. *Infrastructure as a Service* (IaaS);
2. *Platform as a Service* (PaaS);
3. *Software as a Service* (SaaS).

W tabeli 1 zamieszczono podstawową charakterystykę przetwarzania w chmurze według stopnia zaawansowania usług nabywanych przez JSFP.

Udział w tematycznych konferencjach oraz badania własne autorki potwierdziły, że kierownicy JSFP, księgowi i audytorzy od kilku lat bardzo uważnie obserwują dynamiczny rozwój tego typu usług informatycznych. JSFP mają już świadomość, że decydując się na określony model *cloud computing*, muszą przyjąć na siebie ściśle

[23] P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, Ver. 15, 10.07.2009 r., http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, dostęp 15.05.2015; K. Łapiński, B. Wyżnikiewicz, *Raport. Cloud Computing wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski*, Instytut Badań nad Gospodarką Rynkową, Warszawa 2011, s. 5–20.

[24] E.I. Szczepankiewicz, *Audyt kontroli wewnętrznej rachunkowości w środowisku informatycznym*, Difin, Warszawa 2016, s. 66–67.

określony podział między stronami kontroli nad wykorzystywanymi zasobami informatycznymi w chmurze. Podział kontroli zazwyczaj określa usługodawca. W praktyce JSFP rzadko mają możliwość współdecydowania o zakresie podziału kontroli nad swoimi danymi i wykorzystywanymi zasobami informatycznymi. Należy podkreślić, że w tradycyjnym modelu zarządzania zasobami informatycznymi JSFP sprawuje niemal całkowitą kontrolę nad posiadaną przez siebie infrastrukturą, oprogramowaniem i danymi. Jej samowystarczalność i pełna kontrola nad zasobami informatycznymi może być jedynie w niewielkim stopniu ograniczona koniecznością korzystania z usług dostawców łączy internetowych czy serwisu informatycznego.

Tabela 1. Charakterystyka usług *cloud computing*

Usługa	Podstawowa charakterystyka
Infrastructure as a Service	JSFP korzysta za pośrednictwem Internetu z infrastruktury i sprzętu informatycznego (ang. *hardware*). Takim sprzętem może być przestrzeń na wirtualnym dysku internetowym przeznaczona do przechowywania danych albo też wydzierżawione na serwerze miejsce w celu umieszczenia na nim na przykład strony internetowej. Do IaaS zalicza się także korzystanie z mocy obliczeniowej procesorów. W razie potrzeby przeprowadzenia jednorazowej operacji wymagającej ponadstandardowej mocy JSFP może mieć zapewniony dostęp do wirtualnego superkomputera, na który składają się setki połączonych ze sobą procesorów
Platform as a Service	Dla JSFP usługa PaaS jest bardziej zaawansowanym poziomem usługi przetwarzania w chmurze niż usługa IaaS. W tym przypadku JSFP oprócz dostępu do infrastruktury otrzymuje także dostęp do środowiska (w tym platformy programistycznej), w którym może sobie instalować i uruchamiać nowe aplikacje informatyczne. Prostym przykładem takiego środowiska jest system operacyjny Windows. JSFP mogłaby łączyć się poprzez Internet z komputerem, na którym byłby zainstalowany określony system operacyjny i miałaby dostęp do usługi PaaS, czyli mogłaby instalować niezbędne aplikacje. W modelu PaaS instalowane aplikacje pozostają własnością usługobiorcy
Software as a Service	Usługa SaaS dla JSFP jest najbardziej rozbudowanym poziomem *cloud computing*. W modelu tym, oprócz infrastruktury sprzętowej wraz z zawartym środowiskiem operacyjnym, JSFP otrzymuje także dostęp do określonych aplikacji informatycznych, oferowanych przez usługodawcę. Mogą to być proste programy, jak np. edytor tekstu *online*, a także bardziej zaawansowane aplikacje, np. systemy do obsługi księgowości, poczty elektronicznej, rozliczania zamówień. Wówczas JSFP wykorzystuje oprogramowanie należące do usługodawcy, który odpowiada za jego aktualizację i bezawaryjne działanie

Źródło: opracowanie własne na podstawie P. Mell, T. Grance, *The NIST Definition of Cloud Computing*, Ver. 15, 10.07.2009 r., http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf; *The 2011 Cloud Dividend Report*, http://uk.emc.com/microsites/2010/cloud-dividend/index.htm; F. Etro, *Introducing Cloud Computing. Results from a Simulation Study*, International Think-tank on Innovation and Competition, November 2010; P. Dzwonkowski, *Ryzyka związane z usługą przetwarzania danych w chmurze i metody ich łagodzenia*, prezentacja na konferencję „Bezpieczeństwo i Ochrona Danych w Modelu *Cloud Computing*" z dnia 30 marca 2011 r.; K. Łapiński, B. Wyżnikiewicz, *Raport. Cloud Computing wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski*, Instytut Badań nad Gospodarką Rynkową, Warszawa 2011, s. 5–20.

Zatem wybór odpowiedniego modelu przetwarzania w chmurze to wybór pomiędzy stopniem kontroli nad zasobami informatycznymi JSFP a stopniem efektywności ekonomicznej jej działania. Przykładowo, JSFP decydująca się na model *Software as a Service*, nie będzie ponosić kosztów zakupów i utrzymania rozbudowanej infrastruktury informatycznej, ale jej działalność operacyjna jest niemal całkowicie uzależniona od jakości usług dostawcy chmury. Pomimo niższych kosztów zarządzania zasobami informatycznymi przy wykorzystaniu technologii *cloud computing* znacznie rośnie liczba czynników ryzyka dla JSFP.

Stopień zaawansowania przetwarzania w chmurze ma także drugi wymiar, związany z poziomem zarządzania zasobami w chmurze przez usługobiorcę, czyli JSFP. Teoretycy wyróżniają trzy podstawowe modele zarządzania zasobami informatycznymi przez jednostkę w chmurze. Mówi się o modelach:

1) chmury prywatnej,
2) chmury publicznej,
3) chmury hybrydowej.

W praktyce powyższy podział usług przetwarzania w chmurze, zarówno pod względem stopnia zaawansowania nabywanych usług oraz kontroli nad zasobami, jak i fizycznego umiejscowienia chmury (serwery fizycznie zazwyczaj znajdują się w innych krajach), nie jest tak sztywny i nie ogranicza się tylko do trzech modeli wymienianych przez teoretyków. Konieczność dostosowywania się do potrzeb potencjalnego usługobiorcy spowodowała, że obecnie bardzo często są oferowane rozwiązania mieszane. Jednym z takich rozwiązań jest czwarty model wymieniony w tabeli 2, czyli chmura dedykowana, która wykształciła się z modelu chmury hybrydowej. Z usług chmury dedykowanej coraz powszechniej korzystają zarówno jednostki administracji rządowej, jak i jednostki administracji samorządowej.

W tabeli 2 zawarto charakterystykę modeli zarządzania zasobami informatycznymi przez JSFP w chmurze prywatnej, publicznej, hybrydowej i dedykowanej.

Dla osób odpowiedzialnych za rachunkowość JSFP przekazanie niemal całkowitej kontroli nad własnymi zasobami informatycznymi usługodawcom zewnętrznym staje się obecnie warunkiem trudnym do zaakceptowania. Jak potwierdzają wyniki badań przeprowadzonych przez autorkę w 2014 r.[25], osoby odpowiedzialne za rachunkowość nie akceptowały przyjęcia w swoich jednostkach do zarządzania

[25] Badania własne autorka przeprowadziła 25.02.2014 r. podczas konferencji dla członków Stowarzyszenia Księgowych w Polsce, Oddział w Poznaniu, pt.: „Księgowy w epicentrum zmian w VAT, cyfryzacji i globalizacji – wyzwania roku 2014", organizator: Stowarzyszenie Księgowych w Polsce, Oddział w Poznaniu i enova dla biznesu.

zasobami informatycznymi rachunkowości modelu chmury publicznej. Zaledwie 8,5% księgowych deklarowało, że w przyszłości rozważy model chmury dedykowanej lub chmury prywatnej.

Tabela 2. Charakterystyka modeli zarządzania zasobami informatycznymi w chmurze przez JSFP

Usługa	Podstawowa charakterystyka
Chmura prywatna	Całość infrastruktury informatycznej znajduje się fizycznie na terenie kontrolowanym przez JSFP. Jednostka ma więc przez cały czas bezpośredni dostęp do zasobów przechowywanych danych na własnych serwerach posiadających oprogramowanie tworzące chmurę prywatną JSFP. Środowisko informatyczne, w tym oprogramowanie, jest zazwyczaj dopasowane indywidualnie do potrzeb JSFP, która może posiadać wyłączny dostęp do oferowanych w chmurze usług
Chmura publiczna	JSFP w całości może korzystać z zewnętrznych zasobów informatycznych. JSFP sama decyduje, z których usług oferowanych przez usługodawcę będzie korzystać. Jednocześnie JSFP może korzystać za pośrednictwem dostawcy chmury z usług podmiotów trzecich, które nie są bezpośrednim dostawcą chmury, ale dostarczają np. specjalne oprogramowanie, które instaluje się w udostępnionym środowisku operacyjnym dla obsługi chmury. Aspekt braku możliwości kontroli zasobów danych rachunkowości w „chmurze publicznej" przez JSFP obecnie zniechęca księgowych do interesowania się tą usługą. Decydują o tym takie czynniki, jak brak informacji o fizycznym umiejscowieniu chmury (serwery w dowolnym kraju na świecie), a w konsekwencji różne systemy prawne ochrony zasobów informacyjnych i usługobiorców w tych krajach
Chmura hybrydowa	Rozwiązanie to polega na wykorzystywaniu części zasobów informatycznych i przechowywaniu danych w „chmurze prywatnej", a w części w „chmurze publicznej". W „chmurze prywatnej" JSFP przetwarza zazwyczaj na własnych zasobach dane strategiczne i dane prawnie chronione (np. dane niejawne) jednostki. Do „chmury publicznej" JSFP przenosi tylko te aplikacje użytkowe, za pośrednictwem których przetwarza pozostałe dane
Chmura dedykowana w modelu chmury hybrydowej	Jednostka może wykorzystać pełną funkcjonalność chmury w sposób wysoce dopasowany do jej specyficznych potrzeb. Usługodawca dla takiej JSFP wyodrębnia wówczas pewną część chmury (są to specjalnie wydzielone serwery), do której wyłączny dostęp ma tylko ta konkretna JSFP

Źródło: opracowanie własne.

Wyniki uzyskane na podstawie odpowiedzi z ankiet skierowanych przez autorkę do księgowych (67% ankietowanych księgowych zatrudnionych było w sektorze prywatnym i 33% w sektorze finansów publicznych) przedstawiają się następująco:

- tylko 23% ankietowanych księgowych w sektorze prywatnym oraz 49% w JSFP w udokumentowany sposób identyfikuje i ocenia zagrożenia informatyczne, które mogą przeszkodzić realizacji celów i zadań komórki finansowo-księgowej

(np. poprzez sporządzanie rejestru ryzyka, wymaganego standardami kontroli zarządczej w JSFP);
- tylko 19% ankietowanych księgowych w sektorze prywatnym oraz 35% w JSFP potwierdziło, że w przypadku każdego zagrożenia/ryzyka informatycznego został określony poziom ryzyka, jaki można zaakceptować w ich jednostkach;
- 14% ankietowanych księgowych w sektorze prywatnym oraz 44% w JSFP odpowiedziało, że w stosunku do każdego istotnego ryzyka informatycznego został określony sposób radzenia sobie z tym ryzykiem (tzn. zdefiniowano i wdrożono reakcję na ryzyko, wymaganą standardami kontroli zarządczej w JSFP);
- 52% ankietowanych księgowych w sektorze prywatnym oraz 72% w JSFP stwierdziło, że pracownicy w komórce finansowo-księgowej mają bieżący dostęp do procedur/instrukcji ochrony zasobów informatycznych obowiązujących w jednostce (np. poprzez intranet);
- 49% ankietowanych księgowych w sektorze prywatnym oraz 79% w JSFP zapewniało, że w ich jednostkach zostały wdrożone mechanizmy (procedury), służące utrzymaniu ciągłości działalności na wypadek awarii systemu informatycznego oraz zdarzeń losowych związanych z utratą lub zniszczeniem zasobów informatycznych (np. pożaru, powodzi, zalania);
- około 72% wszystkich ankietowanych księgowych uważa, że dokumenty i inne zasoby informatyczne, z których korzystają w swojej pracy, są ich zdaniem chronione przed utratą lub zniszczeniem zgodnie z przepisami;
- 86% ankietowanych księgowych w JSFP oraz 83% w sektorze prywatnym z pośród wszystkich zagrożeń dla bezpieczeństwa informacji najbardziej obawia się prób wyłudzeń danych przez osoby z zewnątrz, w celu dokonywania przelewów z kont jednostki, działań znanych jako *phishing* oraz *spyware*, rozproszonego ataku DoS, w dalszej kolejności ataku wirusów i innych szkodliwych programów, włamania z zewnątrz w celu kradzieży poufnych danych i danych osobowych z publicznych (firmowych) baz danych;
- około 27% wszystkich ankietowanych księgowych za ważne zagrożenia dla bezpieczeństwa (utraty lub zniszczenia) zasobów informatycznych rachunkowości uważa możliwość awarii infrastruktury, sprzętu komputerowego (dysków, serwerów) lub oprogramowania.

Na podstawie kolejnych badań ankietowych przeprowadzonych przez autorkę na przełomie lat 2015–2016 można stwierdzić, że pracownicy w większości badanych JSFP (69% ankietowanych), a w szczególności mniejszych i średnich JSFP (aż 92% ankietowanych) dostrzegli, że aktualnie obowiązujące rozwiązania w systemach

kontroli zarządczej w ich jednostkach nie nadążają za transformacją technologiczną w obszarze IT. Skutkiem tego w wielu obszarach środowiska informatycznego nie zapewniono na właściwym poziomie bezpieczeństwa zasobów informatycznych. Zdaniem 93% ankietowanych w JSFP istnieje niebezpieczeństwo, że podatności na zagrożenia w ich jednostkach w przyszłości mogą zostać wykorzystane przez celowe działania z zewnątrz jednostki. Ponadto w 12% badanych jednostek zdaniem ankietowanych istnieje ryzyko wyrządzenia szkód zasobom informatycznym w wyniku ewentualnych zdarzeń losowych.

5. Podsumowanie

Przegląd literatury[26], analiza regulacji oraz badania empiryczne przeprowadzone przez autorkę potwierdziły, że organizacja i zarządzanie bezpieczeństwem środowiska informatycznego rachunkowości oraz opracowanie, wdrożenie, ocena i doskonalenie systemu kontroli zarządczej w JSFP stanowią obecnie bardzo złożony obszar działań.

Zaprezentowane zagrożenia i wielość czynników je wywołujących pokazują, że obecnie ze względu na dynamiczną transformację technologiczną liczba elementów środowiska informatycznego, które wywołują różne zagrożenia w JSFP, jest coraz większa. Zależnie od przyjętego modelu zarządzania zasobami informatycznymi (model tradycyjny lub model *cloud computing*) kierownictwo JSFP musi uświadomić sobie i przeanalizować znacznie różniące się czynniki ryzyka, które mogą wystąpić w danym środowisku informatycznym i nie może ich zlekceważyć podczas doskonalenia systemu kontroli zarządczej. Kierownictwo JSFP powinno przewidzieć i przeciwdziałać ryzyku, stosując odpowiednie mechanizmy kontroli zarządczej[27], które będą chronić na możliwie najwyższym poziomie zasoby informatyczne przed zagrożeniami, a w konsekwencji przed ich utratą. Wszystkie wyżej omówione czynniki i okoliczności uzasadniają potrzebę bardzo dokładnej analizy podatności poszczególnych elementów na zagrożenia, a także potrzeb jednostki i oczekiwań wobec roli

[26] Literatura zagraniczna nie odnosi się do aspektów kontroli zarządczej w polskim sektorze finansów publicznych. Istnieje natomiast wiele opracowań i specjalistycznych raportów zagranicznych omawiających różne aspekty bezpieczeństwa informacji oraz cyberbezpieczeństwa w szeroko rozumianych organizacjach.

[27] Szerzej o analizie ryzyka dla potrzeb projektowania systemu kontroli E.I. Szczepankiewicz, *Analiza ryzyka jako element systemu kontroli w firmie*, „Biuletyn Rachunkowości" 2008, nr 14.

oraz zadań systemu kontroli zarządczej w środowisku informatycznym rachunkowości. Przy opracowywaniu zasad i środków bezpieczeństwa zasobów informatycznych analizą należy objąć wszystkie wewnętrzne oraz zewnętrzne czynniki ryzyka, które są specyficzne dla danej JSFP[28]. W następstwie przeprowadzonej analizy kierownictwo JSFP powinno przyjąć odpowiednią politykę zarządzania ryzykiem i zasobami w środowisku informatycznym.

Bibliografia

1. Dudek E., *Zagrożenia występujące w środowisku informatycznym rachunkowości*, „Monitor Rachunkowości i Finansów" 2003, nr 7–8.
2. Dzwonkowski P., *Ryzyka związane z usługą przetwarzania danych w chmurze i metody ich łagodzenia*, prezentacja na konferencję „Bezpieczeństwo i Ochrona Danych w Modelu *Cloud Computing*" z dnia 30 marca 2011 r.
3. Etro F., *Introducing Cloud Computing. Results from a Simulation Study*, International Think-tank on Innovation and Competition, November 2010.
4. Fisher R.P., *Information Systems Security*, Prentice-Hall, Englewood Cliffs 1984.
5. Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Helion, Gliwice 1999.
6. Komunikat nr 2 Ministra Finansów z dnia 17 czerwca 2013 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych (Dz.Urz. Min. Fin. z 2013 r., poz. 15).
7. Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych (Dz.Urz. Min. Fin. 2009, nr 15, poz. 84).
8. Łapiński K., Wyżnikiewicz B., *Raport. Cloud Computing wpływ na konkurencyjność przedsiębiorstw i gospodarkę Polski*, Instytut Badań nad Gospodarką Rynkową, Warszawa 2011.
9. Mell P., Grance T., *The NIST Definition of Cloud Computing*, Ver. 15, 10.07.2009 r., http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, dostęp 15.05.2015.
10. *Międzynarodowe Standardy Rewizji Finansowej 1996*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 1996.
11. *Międzynarodowe Standardy Rewizji Finansowej 2005. Wydanie zbiorcze obejmujące regulacje z zakresu rewizji finansowej, usług atestacyjnych i etyki*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 2005.

[28] Szerzej o tym ryzyku: E.I. Szczepankiewicz, *Jak chronić dane finansowe w środowisku informatycznym rachunkowości*, „Biuletyn Rachunkowości i Finansów" 2007, nr 8(32), s. 61–64.

12. *Międzynarodowe Standardy Rewizji Finansowej i Kontroli Jakości: 210, 220, 240, 250, 265, 300, 315, 320, 402, 450, 800, 805, 810*, t. 3, IFAC, tłumaczenie: Krajowa Izba Biegłych Rewidentów i Stowarzyszenie Księgowych w Polsce, Warszawa 2010.
13. *Międzynarodowe Standardy Rewizji Finansowej i Międzynarodowe Wskazówki dotyczące Praktyki Rewizji Finansowej 2001*, IFAC, tłumaczenie: Stowarzyszenie Księgowych w Polsce, Warszawa 2001.
14. Mitnick K., Simon W., *Łamałem ludzi, nie hasła. Sztuka podstępu*, Helion, Gliwice 2002.
15. PN-I-02000:2002. *Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia.*
16. PN-ISO/IEC 17799/2007. *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.*
17. PN-ISO/IEC 20000–1:2014–01. *Technika informatyczna. Zarządzanie usługami. Część 1: Wymagania dla systemu zarządzania usługami.*
18. PN-ISO/IEC 20000–2:2007. *Technika informatyczna. Zarządzanie usługami. Część 2: Reguły postępowania.*
19. PN-ISO/IEC 2382–8:2001. *Technika informatyczna. Terminologia. Część 8: Bezpieczeństwo.*
20. PN-ISO/IEC 24762:2010. *Technika informatyczna. Techniki bezpieczeństwa. Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.*
21. PN-ISO/IEC 27001:2007. *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*
22. PN-ISO/IEC 27005:2014–01. *Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.*
23. Raport Techniczny ISO/IEC TR 13335–3/1998. *Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Techniki zarządzania bezpieczeństwem systemów informatycznych.*
24. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 5 czerwca 2014 r. w sprawie zasad potwierdzania, przedłużania ważności, unieważniania oraz wykorzystania profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz.U. z 2014, poz. 778 ze zm.).
25. Rozporządzenie Ministra Finansów z dnia 26 kwietnia 2012 r. zmieniające rozporządzenie w sprawie określenia rodzajów deklaracji, które mogą być składane za pomocą środków komunikacji elektronicznej (Dz.U. z 2012 r., poz. 474 ze zm.).
26. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 2 listopada 2007 r. w sprawie systemów teleinformatycznych stosowanych w jednostkach organizacyjnych pomocy społecznej (Dz.U. z 2007 r. nr 216, poz. 1609 ze zm.).

27. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., nr 100, poz. 1024 ze zm.).
28. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 25 kwietnia 2014 r. zmieniające rozporządzenie w sprawie trybu dostępu i wzoru upoważnienia do dostępu do Krajowego Systemu Informatycznego (KSI) oraz wykorzystywania danych (Dz.U. z 2014 r., poz. 558 ze zm.).
29. Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz.U. z 2004 r. nr 100, poz. 1023 ze zm.).
30. Rozporządzenie Ministra Sprawiedliwości z dnia 29 grudnia 2011 r. w sprawie trybu zakładania konta w systemie teleinformatycznym, sposobu korzystania z systemu teleinformatycznego i podejmowania w nim czynności związanych z zawiązaniem spółki z ograniczoną odpowiedzialnością przy wykorzystaniu wzorca umowy oraz wymagań dotyczących podpisu elektronicznego (Dz.U. z 2011 r. nr 297, poz. 1762 ze zm.).
31. Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. z 1999 r. nr 18, poz. 162 ze zm.).
32. Rozporządzenie Prezesa Rady Ministrów z dnia 8 maja 2014 r. zmieniające rozporządzenie w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2014 r., poz. 590 ze zm.).
33. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r., poz. 526 ze zm.).
34. Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty i warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. z 2002 r. nr 128, poz. 1094 ze zm.).
35. Szczepankiewicz E.I., *Jak chronić dane finansowe w środowisku informatycznym rachunkowości*, „Biuletyn Rachunkowości i Finansów" 2007, nr 8(32).

36. Szczepankiewicz E.I., *Wybrane procedury kontroli wewnętrznej w środowisku informatycznym rachunkowości*, w: *Rachunkowość w teorii i praktyce*, t. I, *Rachunkowość finansowa*, red. W. Gabrusewicz, Wydawnictwo Akademii Ekonomicznej w Poznaniu, Poznań 2007.
37. Szczepankiewicz E.I., *Analiza ryzyka jako element systemu kontroli w firmie*, „Biuletyn Rachunkowości" 2008, nr 14.
38. Szczepankiewicz E.I., *Jakie są zasady opracowywania procedur kontrolnych w firmie*, „Biuletyn Rachunkowości" 2008, nr 12(60).
39. Szczepankiewicz E.I., *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych*, red. W. Gabrusewicz, PWE, Warszawa 2010, s. 198.
40. Szczepankiewicz E.I., *Audyt sprawozdań finansowych w środowisku informatycznym*, w: *Audyt sprawozdań finansowych. Teoria i praktyka*, red. W. Gabrusewicz, PWE, Warszawa 2014.
41. Szczepankiewicz E.I., *Audyt kontroli wewnętrznej rachunkowości w środowisku informatycznym*, Difin, Warszawa 2016.
42. Szczepankiewicz E.I., *Kontrola zarządcza w jednostkach samorządu terytorialnego. Doskonalenie procedur kontroli zarządczej w środowisku informatycznym rachunkowości*, Wydawnictwo Naukowe CONTACT, Poznań 2016.
43. Szczepankiewicz E.I., *Zasady i procedury kontroli zarządczej w obszarze systemów informatycznych rachunkowości w jednostkach sektora finansów publicznych*, Wydawnictwo Naukowe CONTACT, Poznań 2016.
44. Szczepankiewicz E.I., Dudek M., *Rozwój technologii informatycznych a zagrożenia i zarządzanie bezpieczeństwem informacji w przedsiębiorstwach*, w: *Logistyka – Komunikacja – Bezpieczeństwo, Wybrane problemy*, red. M. Grzybowski, J. Tomaszewski, Wydawnictwo Wyższej Szkoły Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni, Gdynia 2009.
45. *The 2011 Cloud Dividend report*, http://uk.emc.com/microsites/2010/cloud-dividend/index.htm (dostęp 12.02.2016).
46. Ustawa z 6 czerwca 1997 r. Kodeks karny (Dz.U. z 1997 r. nr 55, poz. 553 z późn. zm.).
47. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2013 r., poz. 235 ze zm.).
48. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r. nr 144, poz. 1204 ze zm.).
49. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2013 r., poz. 262 ze zm.).
50. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 1997 r. nr 114, poz. 740 ze zm.).

51. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. z 2001 r. nr 128, poz. 1402 ze zm.).
52. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (tj. Dz.U. z 2016 r., poz. 1870 ze zm.).
53. Ustawa z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa oraz o zmianie niektórych ustaw (Dz.U. z 2013 r., poz. 194 ze zm.).
54. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. nr 101, poz. 926 ze zm.).
55. Wójcik J.W., *Przestępstwa komputerowe*, cz. 1, *Fenomen cywilizacji*, CIM, Warszawa 1999.
56. Wójcik J.W., *Przestępstwa komputerowe*, cz. 2, *Techniki zapobiegania*, CIM, Warszawa 1999.

Threats to Accounting IT Resources at the Age of Information Technology Transformation in the Public Finance Entities

Summary

An important aspect of the appropriate level of efficiency and quality of operation in the entities of public finance is to ensure the continuity of IT operation and security of IT resources. The use of IT systems and teleinformation technology in these entities is connected with numerous threats related to the IT environment. The article discusses the most important threats with regard to a traditional model of IT resources management in entities and a new model of cloud computing. It mentions the problem of threats and conclusions from the research in the context of technological transformations as well as imperfectness of management control systems, which do not always keep up with these changes. The research method used in the study is the review of the literature, legal regulations, management control standards, internal audit standards, ISO norms as well as drawing conclusions.

Keywords: accounting, IT system, threats, IT resources security, risk management, management control system, cloud computing